Defense Information Systems Agency
Department of Defense

Department of Defense Information Assurance Range:
A Venue for Test and Evaluation In Cyberspace

DISA-JITC/JTG1
August 2011

UNCLASSIFIED

Agenda

- **Information Assurance (IA) Range**
  - **IA Range Drivers**
  - **Department of Defense (DOD) Range Initiatives**
  - **IA Range Mission Pillars and Objectives**
    - **Test and Evaluation (T&E) Mission Pillar and Objectives**
  - **IA Range Recent Success Stories**
  - **IA Range Status and Way Ahead**
  - **Points of Contact**

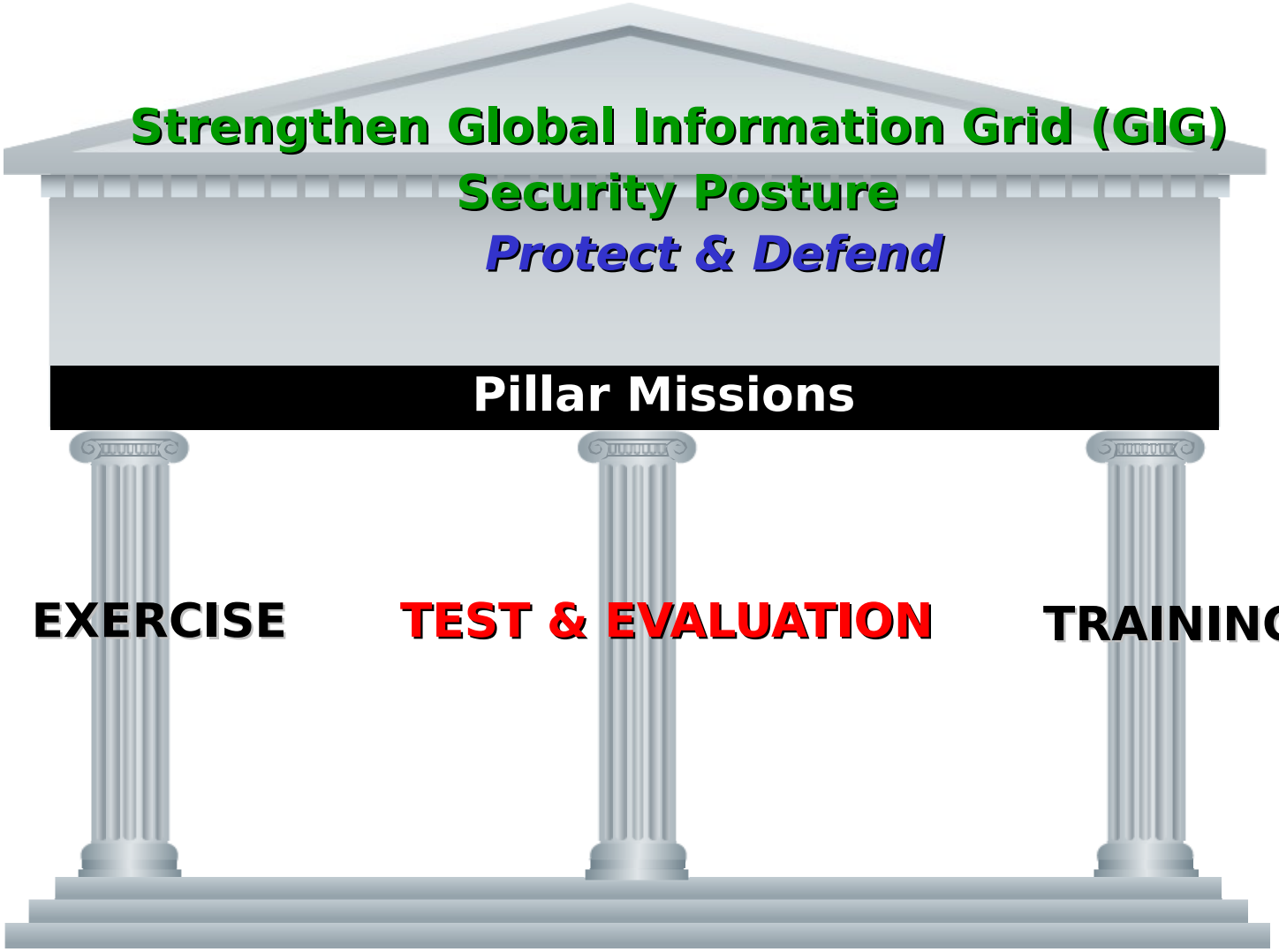
DOD IA Range Drivers

- **Comprehensive National Cybersecurity Initiative (CNCI)**
  - **NSPD-54 / HSPD-23**
  - **IA Range (Initiative 7)**
  - **Federal & national exercise program (Initiative 8)**
- **DOD IA Strategy (Goal 5): An IA workforce able to…**
  - **Effectively employ IA tools, techniques and strategies to defeat adversaries**
  - **Proactively identify and mitigate the full spectrum of rapidly evolving threats to defend the Net**
- **National Military Strategy for Cyberspace**
  - **Robust exercising with increased realism**
- **Need for DOD network defenders to learn to "*Train as we Fight*"**
  - **Protect and defend against specific threat generations**

DOD Range Initiatives

LABEL	IA RANGE	IO RANGE	DARPA NCR
Classification	Unclassified	Multi level, up to TS/SCI & SAP/SAR	Multiple levels of security
Audience	DOD IA/CND Practitioners	COCOMS, Services, Interagency, Coalition and Test & Eval Organizations	Researchers
Environment	Today's Global Information Grid (GIG) – IA/CND	"Closed loop" fully meshed network & management among connected nodes	Tomorrow's environment
Functions	Provides test, training, and exercising environment, modeled after the GIG and joint services architecture	Provides secure connectivity, resource allocation, event coordination and access to actual and modeled tools and targets	Provides a simulated, emulated, and replicated research environment to support experiments
	Test and evaluate near-term tools; pilot shrink-wrapped products prior to acquisition	Provides security, connectivity and network management to event participants' capabilities	Proof of concept for emerging/future capabilities
	Exercise and assess personnel and TTPs	Access to IO tools/targets to provide exposure to and validation of IO capabilities in tests, training and exercises	Advanced research of tomorrow's cyber issues and capabilities focused at the national level
Depth of Operation	Normal operations to Level 2 attack conditions	Does not own capabilities, rather a means to interconnect capabilities from distributed locations	Sophisticated & highly adversarial attack conditions
Provides	Integration of current DOD technologies, people, policies, and procedures	IO Range provides highly secure access to current and developmental IO capabilities and target environments	Research & development of revolutionary technologies

IA Range Mission Pillars



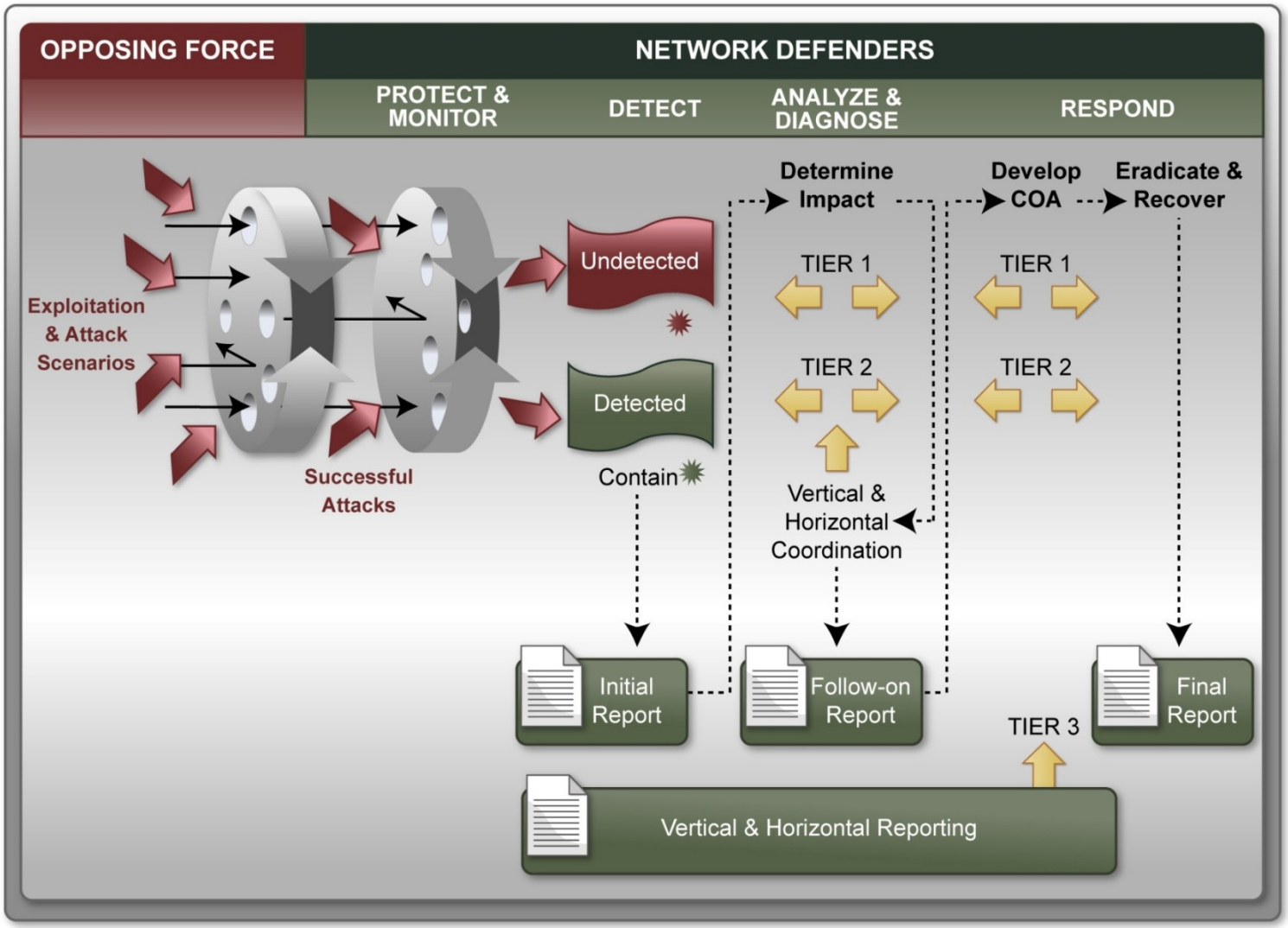
UNCLASSIFIED

Test & Evaluation Objectives

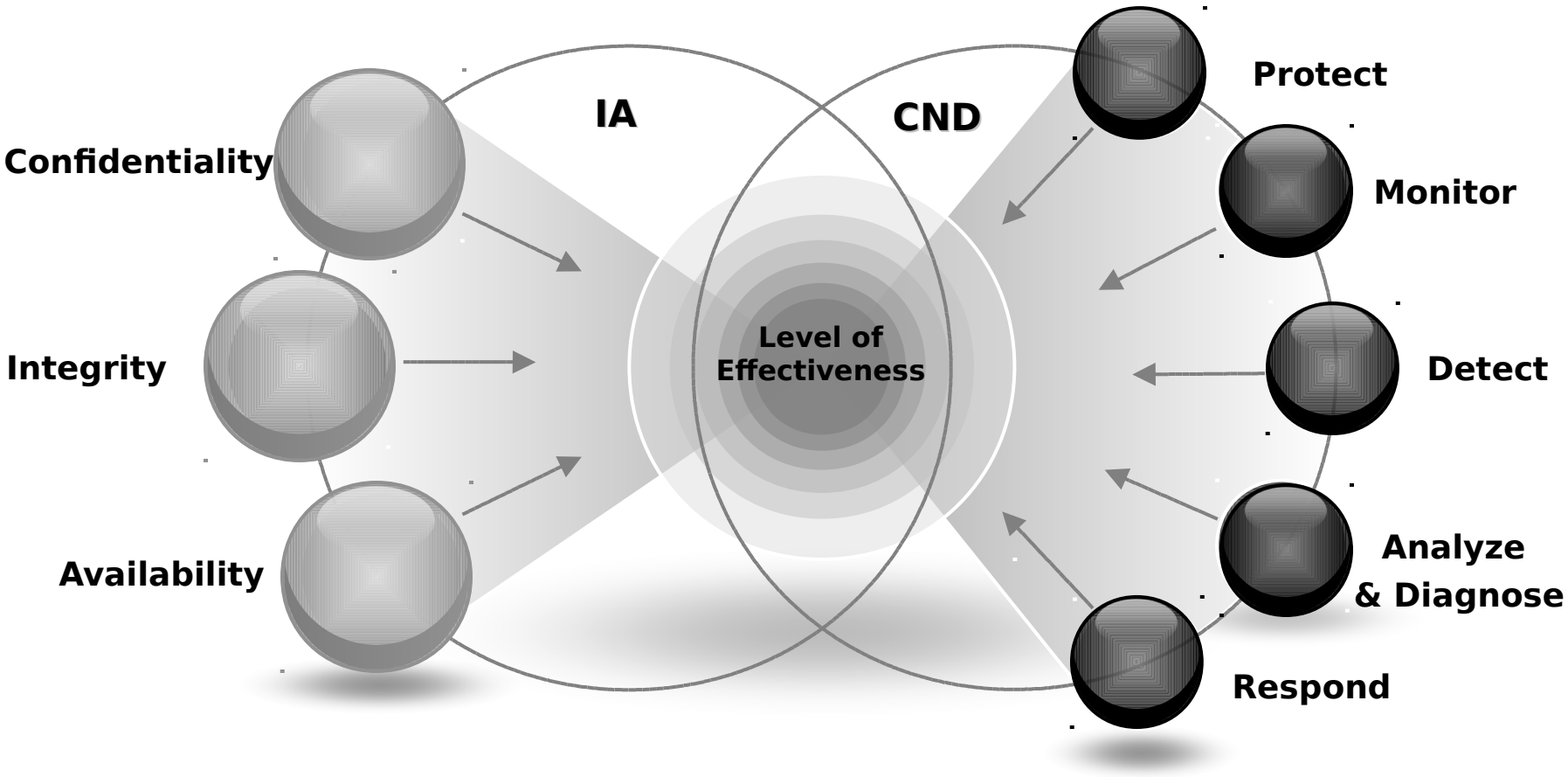
- **The IA Range framework promotes a consistent, repeatable, and verifiable T&E venue by which IA and Computer Network Operations (CNO) technical and operational concepts will be validated against requirements and specifications for improvement.**

- **The IA Range will seek to achieve the following T&E objectives:**
  - **Improve Cyber Security Workforce Operational Performance**
  - **Validate Capabilities and Services Provided by CND Tools and Mechanisms**
  - **Validate and Improve CND Tactics, Techniques, and Procedures**
  - **Validate Acceptable Level of Service of Computer Network Defense Service Providers (CNDSPs)**
  - **Validate IA Mitigation Strategies for Program of Records**

Improve Cybersecurity Workforce Operational Performance



Validate Capabilities and Services Provided by CND Tools and Mechanisms



Validate and Improve CND TTPs

Adequate documentation of actions (and methods) to implement and manage technology

Promotes a balanced integration of *people*, *operations*, and *technology* to meet day-to-day operational priorities

People

- **Proper management and deployment of technologies and methods**
- **Understanding of assigned roles and responsibilities**

Operations

- **Adherence to principles of commonality, standardization, and operational ease of use**
- **Consistent and effective set of expectations to guide day-to-day operations**

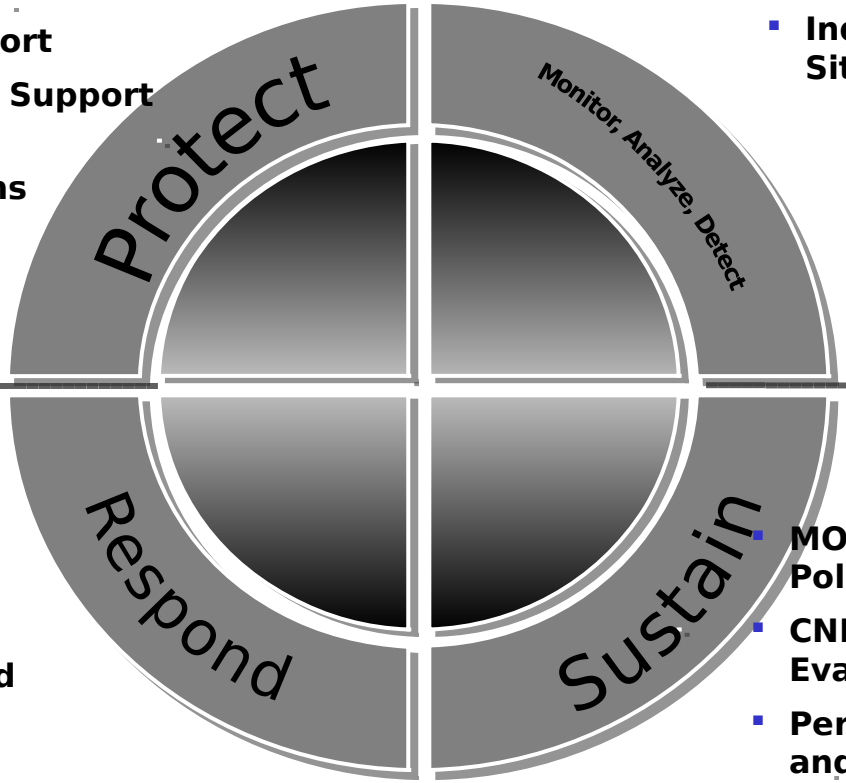
Technology

- **Supports the procurement and deployment of new technology**

Validate Acceptable Level of Service of CNDSPs

- Vulnerability Analysis and Assessment (VAA) Support
- Information Assurance Vulnerability Management (IAVM)
- Virus Protection Support
- Subscriber Protection Support and Training
- Information Operations Condition (INFOCON) Implementation
- CND Red Teaming

- Network Security Monitoring/Intrusion Detection
- Attack Sensing & Warning (AS&W)
- Indications & Warning (I&W) / Situational Awareness



- Incident Reporting
- Incident Response and Analysis

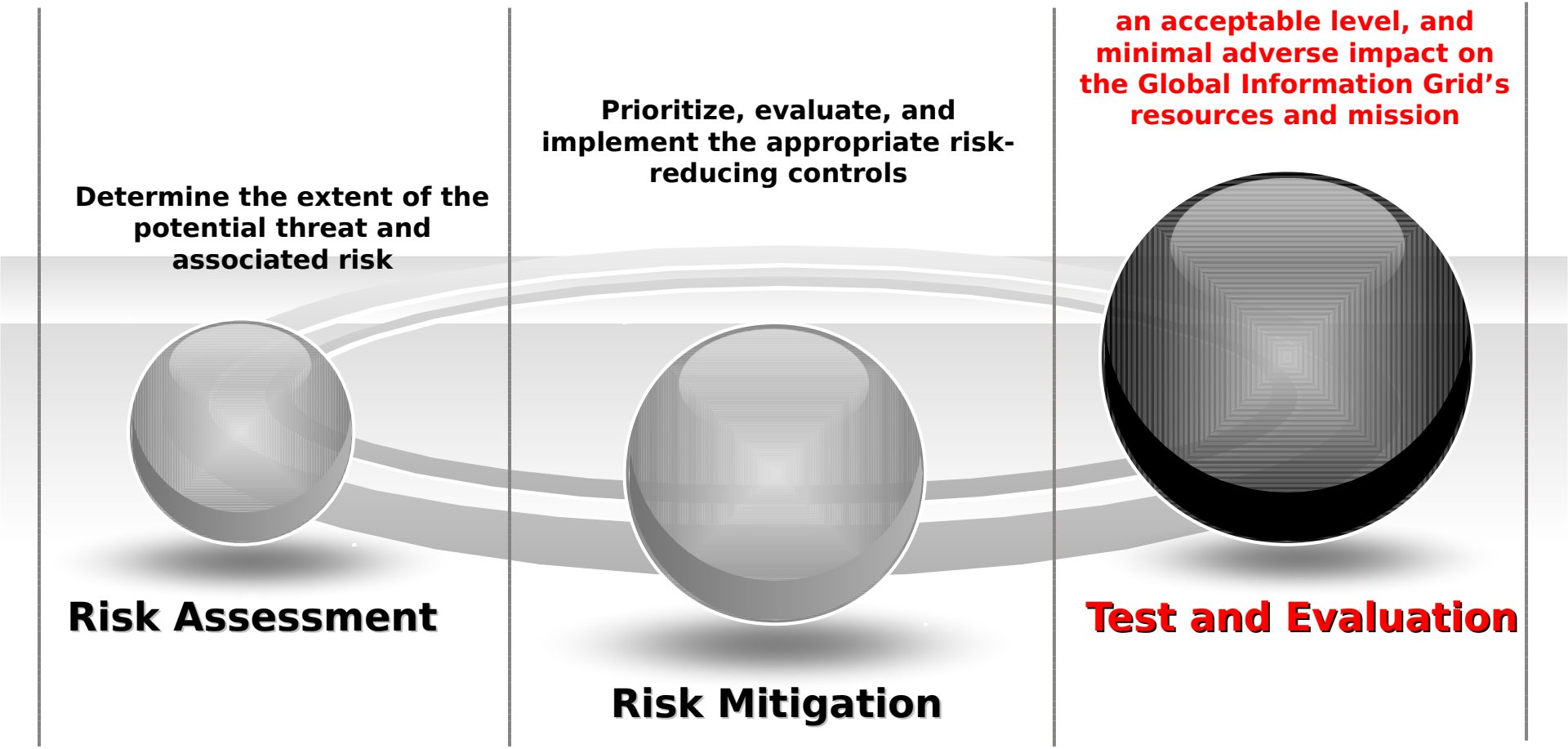
- MOUs and Contracts, CND Policies and Procedures
- CND Technology Development, Evaluation and Implementation
- Personnel Levels and Training and Certification
- Security Administration
- Primary CNDS Provider Information Systems

Validate IA Mitigation Strategies for Program of Records

Determine the extent of the potential threat and associated risk

Prioritize, evaluate, and implement the appropriate risk-reducing controls

Validate least cost-approach, decrease of mission risk to an acceptable level, and minimal adverse impact on the Global Information Grid's resources and mission



Risk Assessment

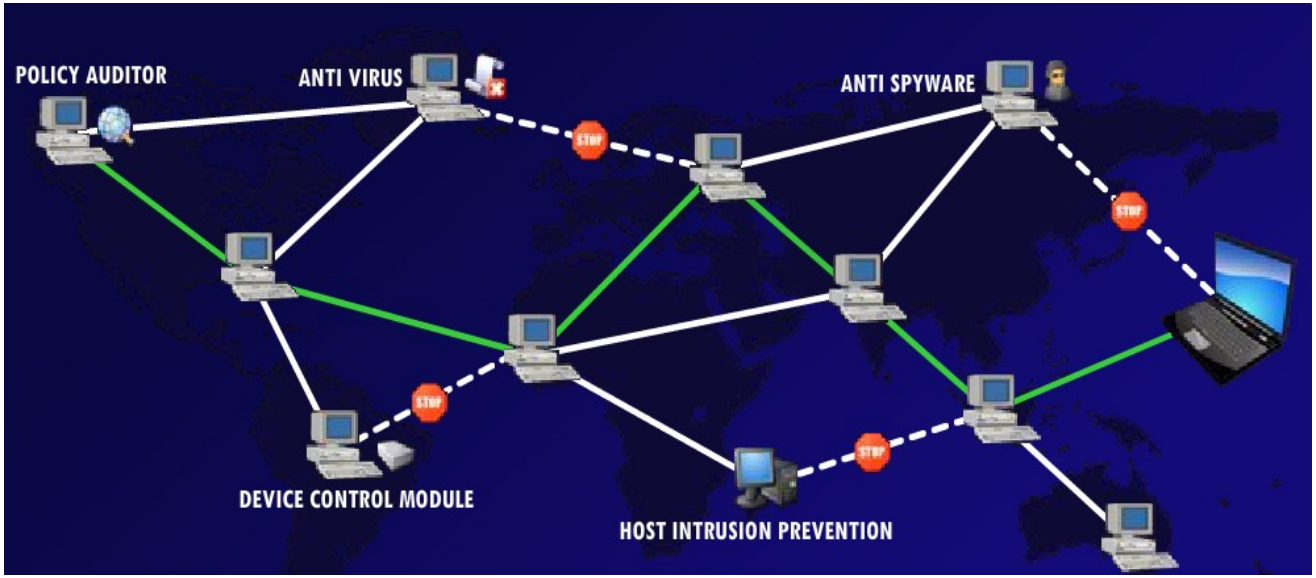
Risk Mitigation

Test and Evaluation

Recent Success Stories

The DOD IA Range sponsored the Host Based Security System (HBSS) Quick Reaction Test (QRT)

January 6, 2010 – January 5, 2011



Under the authority of the Department of Defense Instruction (DODI) 5010.41, *Joint Test and Evaluation Program*, the HBSS QRT tested and developed Concept of Operations (CONOPS) and Tactics, Techniques, and Procedures (TTPs) for the employment of personnel and equipment that resulted in standard configurations and tactics for the implementation and operation of HBSS throughout the Global Information Grid.

IA Range Status and Way Ahead

- **IA Range Status**
  - **IA Range met its Initial Operational Capability objectives**
    - **Provides a foundational environment to educate, equip, and exercise IA and CNO**
    - **Provides an initial suite of services to include of Web, e-mail, Domain Name System, Voice over Internet Protocol, Instant Messaging, and Internet**
    - **Provides GIG transfer infrastructure by supporting the connection of separate CC/S/A and field activities ISs to meet common-user and special purpose information transfer requirements**
- **Way Ahead**
  - **Projected Activities**
    - **Methodical integration of selected DISA and NSA Tier 1 Global Network Defense (GND) mechanisms and capabilities to emulate GND technical and operational capabilities (today's GIG IA architecture within a NetOps framework) .**
    - **DISA is studying the possibility to physically move the IA Range from its pilot environment to its production environment (government facility)**

Points of Contact

- **Mr. Timothy Holmes, JITC IA Branch Technical Advisor**
  - **Kevin.Holmes@disa.mil**
  - **(301) 744-5512 DSN: 354**
- **Mr. Gordon Bass, DOD IA Range Program Manager**
  - **Gordon.Bass@disa.mil**
  - **(301) 225-3220 DSN: 312**

DISA

UNCLASSIFIED